RFC 2630: S/MIME v3 Cryptographic Message Syntax

References:

RFC 1321, The MD5 Message-Digest Algorithm
RFC 2268, A Description of the RC2 (r) Encryption Algorithm
RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2630, Cryptographic Message Syntax
RFC 2631, Diffie-Hellman Key Agreement Method
FIPS Pub 180-1, Secure Hash Standard
FIPS Pub 186, Digital Signature Standard

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the implementation include the protection content, ContentInfo, and implement the data, signed-data, and enveloped-data content types? [RFC 2630 2]		
Are signed attributes and authenticated attributes transmitted in DER form (to ensure that recipients can verify a content that contains one or more unrecognized attributes)? [RFC 2630 2]		
Does the CMS have the following ASN.1 type? ContentInfo: ContentInfo ::= SEQUENCE { contentType ContentType, content [0] EXPLICIT ANY DEFINED BY contentType } ContentType ::= OBJECT IDENTIFIER [RFC 2630 3]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the signed-data content type have the following ASN.1 type? SignedData ::= SEQUENCE { version CMSVersion, digestAlgorithms DigestAlgorithmIdentifiers, encapContentInfo EncapsulatedContentInfo, certificates [0] IMPLICIT CertificateSet OPTIONAL, crls [1] IMPLICIT CertificateRevocationLists OPTIONAL, signerInfos SignerInfos } DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier SignerInfos ::= SET OF SignerInfo [RFC 2630 5.1]		
For the SignedData content type, if no attribute certificates are present in the certificates field, the encapsulated content type is id-data, and all of the elements of SignerInfos are version 1, then is the value of “version” 1? [RFC 2630 5.1]		
For the SignedData content type, if attribute certificates are present, the encapsulated content type is other than id-data, or any of the elements of SignerInfos are version 3, then is the value of “version” 3? [RFC 2630 5.1]		
For the SignerInfo content type, if the SignerIdentifier is the CHOICE issuerAndSerialNumber, then is the “version” 1? [RFC 2630 5.3]		
For the SignerInfo content type, if the SignerIdentifier is subjectKeyIdentifier, then is the “version” 3? [RFC 2630 5.3]		
For the SignerInfo content type, if the content type of the EncapsulatedContentInfo value being signed is not id-data, is the signedAttributes field present? [RFC 2630 5.3]		
For the SignerInfo content type, is each SignedAttribute in the SET DER encoded? [RFC 2630 5.3]		
For the SignerInfo content type, if the SignedAttribute field is present, does it contain, at a minimum, the following two attributes? A content-type attribute having as its value the content type of the EncapsulatedContentInfo value being signed A message-digest attribute, having as its value the message digest of the content. [RFC 2630 5.3, 5.4]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is the message digest value calculated by the recipient the same as the value of the messageDigest attribute included in the signedAttributes of the signedData signerInfo? [RFC 2630 5.6]		

Does the enveloped-data content type have the following ASN.1 type?
EnvelopedData:
EnvelopedData ::= SEQUENCE {
version CMSVersion,
originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
encryptedContentInfo EncryptedContentInfo,
unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL }
OriginatorInfo ::= SEQUENCE {
certs [0] IMPLICIT CertificateSet OPTIONAL,
crls [1] IMPLICIT CertificateRevocationLists OPTIONAL }
RecipientInfos ::= SET OF RecipientInfo
EncryptedContentInfo ::= SEQUENCE {
contentType ContentType,
contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }
EncryptedContent ::= OCTET STRING
UnprotectedAttributes ::= SET SIZE (1..MAX) OF Attribute
[RFC 2630 6.1]		

For the enveloped-data content type, if originatorInfo is present, then is the “version” 2? [RFC 2630 6.1]		
For the enveloped-data content type, if any of the RecipientInfo structures included have a version other than 0, then is the “version” 2? [RFC 2630 6.1]		
For the enveloped-data content type, if unprotectedAttrs is present, then is the “version” 2? [RFC 2630 6.1]		
For the enveloped-data content type, if originatorInfo is absent, all of the RecipientInfo structures are version 0, and unprotectedAttrs is absent, then is the “version” 0? [RFC 2630 6.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For the enveloped-data content type, is there at least one element in the recipientInfos field? [RFC 2630 6.1]		
For the enveloped-data content type, if the optional encryptedContent field is not present, is its intended value supplied by other means? [RFC 2630 6.1]		
For the KeyTransReceiptInfo content type, if the RecipientIdentifier is the CHOICE issuerAndSerialNumber, then is the “version” 0? [RFC 2630 6.2.1]		
For the KeyTransReceiptInfo content type, if the RecipientIdentifier is subjectKeyIdentifier, then is the “version” 2? [RFC 2630 6.2.1]		
Does the recipient's certificate contain a key transport public key? [RFC 2630 6.2.1]		
For the KeyAgreeReceiptInfo content type, is the “version” field of KeyAgreeReceiptInfo 3? [RFC 2630 6.2.2]		
Does the recipient's certificate contain a key agreement public key? [RFC 2630 6.2.2]		
For the KEKReceiptInfo content type, is the “version” field of KEKRecipientInfo 4? [RFC 2630 6.2.3]		
For content-encryption algorithms that assume the input length is a multiple of k octets, where k is greater than one, is the input padded at the trailing end with k-(lth mod k) octets all having value k-(lth mod k), where lth is the length of the input? [RFC 2630 6.3]		
Does the digested-data content type have the following ASN.1 type? DigestedData: DigestedData ::= SEQUENCE { version CMSVersion, digestAlgorithm DigestAlgorithmIdentifier, encapContentInfo EncapsulatedContentInfo, digest Digest } Digest ::= OCTET STRING [RFC 2630 7]		
For the digested-data content type, if the encapsulated content type is id-data, then is the value of “version” 0? [RFC 2630 7]		
For the digested-data content type, if the encapsulated content type is other than id-data, then is the value of “version” 2? [RFC 2630 7]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For the encrypted-data content type, are keys managed by other means? (I.e., Keys are not managed in the same manner as enveloped-data content keys). [RFC 2630 8]		
Does the encrypted-data content type have the fololowing ASN.1 type? EncryptedData: EncryptedData ::= SEQUENCE { version CMSVersion, encryptedContentInfo EncryptedContentInfo, unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL } [RFC 2630 8]		
For the encrypted-data content type, if unprotectedAttrs is present, then is the “version” 2? [RFC 2630 8]		
For the encrypted-data content type, if unprotectedAttrs is absent, then is the ‘version” 0? [RFC 2630 8]		
Does the authenticated-data content type shall have the following ASN.1 type? AuthenticatedData: AuthenticatedData ::= SEQUENCE { version CMSVersion, originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL, recipientInfos RecipientInfos, macAlgorithm MessageAuthenticationCodeAlgorithm, digestAlgorithm [1] DigestAlgorithmIdentifier OPTIONAL, encapContentInfo EncapsulatedContentInfo, authenticatedAttributes [2] IMPLICIT AuthAttributes OPTIONAL, mac MessageAuthenticationCode, unauthenticatedAttributes [3] IMPLICIT UnauthAttributes OPTIONAL} AuthAttributes ::= SET SIZE (1..MAX) OF Attribute UnauthAttributes ::= SET SIZE (1..MAX) OF Attribute MessageAuthenticationCode ::= OCTET STRING [RFC 2630 9.1]		
For the authenticated-data content type, is the “version” 0? [RFC 2630 9.1]		
For the authenticated-data content type, is there at least one element in the recipientInfos field? [RFC 2630 9.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For the authenticated-data content type, if the digestAlgorithm field is present, then is the authenticatedAttributes field present? [RFC 2630 9.1]		
For the authenticated-data content type, if the content type of the EncapsulatedContentInfo value being authenticated is not id-data , then is the authenticatedAttributes structure present? [RFC 2630 9.1]		
For the authenticated-data content type, if the authenticatedAttributes field is present, then is the digestAlgorithm field present? [RFC 2630 9.1]		
For the authenticated-data content type, is each AuthenticatedAttribute in the SET DER encoded? [RFC 2630 9.1]		
For the authenticated-data content type, if the authenticatedAttributes field is present, then does it must contain, at a minimum, the following two attributes: A content-type attribute having as its value the content type of the EncapsulatedContentInfo value being authenticated. A message-digest attribute, having as its value the message digest of the content? [RFC 2630 9.1]		
In the MAC generation process, if the authenticatedAttributes field is present, then is the content-type attribute and the message-digest attribute included, and the input to the MAC calculation process the DER encoding of authenticatedAttributes? [RFC 2630 9.2]		
In the MAC verification process, is the message MAC value calculated by the recipient the same as the value of the MAC field? [RFC 2630 9.3]		
In the MAC verification process when the authenticatedAttributes field is present, is the content message digest value calculated by the recipient the same as the message digest value included in the authenticatedAttributes message-digest attribute? [RFC 2630 9.3]		
Is the OtherKeyAttribute type attribute object identifier registered along with the syntax of the attribute itself? [RFC 2630 10.2.7]		
If present, does the content-type attribute have a single attribute value (i.e., no zero or multiple instances of AttributeValue)? [RFC 2630 11.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For the content-type attribute type, does the SignedAttributes in signerInfo include zero or one instances of the content-type attribute? [RFC 2630 11.1]		
For the content-type attribute type, does the AuthAttributes in AuthenticatedData include zero or one instances of the content-type attribute? [RFC 2630 11.1]		
Is the message-digest attribute a signed attribute or an authenticated attribute? [RFC 2630 11.2]		
Does the message-digest attribute have a single attribute value? [RFC 2630 11.2]		
For the message-digest attribute type, does the SignedAttributes in signerInfo include zero or one instances of the message-digest attribute? [RFC 2630 11.2]		
For the signing-time attribute type, are dates between 1 January 1950 and 31 December 2049 (inclusive) encoded as UTCTime? [RFC 2630 11.3]		
For the signing-time attribute type, are dates with year values before 1950 or after 2049 encoded as GeneralizedTime? [RFC 2630 11.3]		
For the signing-time attribute type, are UTCTime values expressed in Greenwich Mean Time (Zulu) and does the value include seconds (i.e., times are YYMMDDHHMMSSZ), even where the number of seconds is zero? [RFC 2630 11.3]		
For the signing-time attribute type, is midnight (GMT) represented as "YYMMDD000000Z"? [RFC 2630 11.3]		
For the signing-time attribute type, is the century determined as follows? Where YY is greater than or equal to 50, the year shall be interpreted as 19YY; and Where YY is less than 50, the year shall be interpreted as 20YY [RFC 2630 11.3]		
For the signing-time attribute type, are GeneralizedTime values expressed in Greenwich Mean Time (Zulu) and do they include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero? [RFC 2630 11.3]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For the signing-time attribute type, do GeneralizedTime values not include fractional seconds? [RFC 2630 11.3]		
Does the signing-time attribute have a single attribute value, even though the syntax is defined as a SET OF AttributeValue? (I.e., there must not be zero or multiple instances of AttributeValue present.) [RFC 2630 11.3]		
For the signing-time attribute type, does the SignedAttributes in a signerInfo not include multiple instances of the signing-time attribute? [RFC 2630 11.3]		
Is the countersignature attribute an unsigned attribute; and therefore not a signed attribute, an authenticated attribute, or an unauthenticated attribute? [RFC 2630 11.4]		
Does the signedAttributes field contain a message-digest attribute if it contains any other attributes? [RFC 2630 11.4]		
For the countersignature attribute, are there one or more instances of AttributeValue present? [RFC 2630 11.4]		
Does the CMS implementation include SHA-1 as a digest algorithm? [RFC 2630 10.1, 12.1; FIPS Pub 180-1]		
Does the CMS implementation also include MD5 as a digest algorithm? [RFC 2630 12.1]		
If present, does the SHA-1 AlgorithmIdentifier parameters field contain an ASN.1 NULL? [RFC 2630 12.1.1]		
If the MD5 algorithm is supported , is AlgorithmIdentifier parameters field present, and does it contain NULL? [RFC 2630 12.1.2; RFC 1321 1.0]		
Does the CMS implementations include DSA as the signature algorithm? [RFC 2630 10.1, 12.2]		
Does the CMS implementations also include RSA as a signature algorithm? [RFC 2630 12.2]		
For the DSA signature algorithm,is the AlgorithmIdentifier parameters field **not** present? [RFC 2630 12.2.1, FIPS Pub 186]		
Does the CMS implementation include key agreement using X9.42 Ephemeral-Static Diffie-Hellman? [RFC 2630 10.1, 12.3.1; RFC 2631]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Are all symmetric encryption algorithms that the CMS implementation includes as a content-encryption algorithm also included as a key-encryption algorithm? [RFC 2630 12.3.1]		
Does the CMS implementation include key agreement of Triple-DES pairwise key-encryption keys and Triple-DES wrapping of Triple-DES content-encryption keys? [RFC 2630 12.3.1]		
Does the CMS implementation also include key agreement of RC2 pairwise key-encryption keys and RC2 wrapping of RC2 content-encryption keys? [RFC 2630 12.3.1]		
For key agreement of RC2 key-encryption keys, are 128 bits generated as input to the key expansion process used to compute the RC2 effective key? [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The “version” is 3. [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The originator is the originatorKey alternative. [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The originatorKey algorithm fields contain the dh-public-number object identifier with absent parameters. [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The originatorKey publicKey field contains the sender's ephemeral public key. [RFC 2630 12.3.1, RFC 2268]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The keyEncryptionAlgorithm is the id-alg-ESDH algorithm identifier. [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The algorithm identifier parameter field for id-alg-ESDH is KeyWrapAlgorihtm, and this parameter is present. [RFC 2630 12.3.1, RFC 2268]		
When using Ephemeral-Static Diffie-Hellman, are the EnvelopedData RecipientInfos KeyAgreeRecipientInfo and AuthenticatedData RecipientInfos KeyAgreeRecipientInfo fields used as follows? The RecipientEncryptedKey KeyAgreeRecipientIdentifier contains either the issuerAndSerialNumber identifying the recipient's certificate or the RecipientKeyIdentifier containing the subject key identifier from the recipient's certificate. In both cases, the recipient's certificate contains the recipient's static public key and the RecipientEncryptedKey EncryptedKey contains the content-encryption key encrypted with the Ephemeral-Static Diffie-Hellman generated pairwise key-encryption key using the algorithm specified by the KeyWrapAlgortihm. [RFC 2630 12.3.1, RFC 2268]		
Do RSA implementations include key transport of Triple-DES content-encryption keys? [RFC 2630 12.3.2]		
For the RSA key transport algorithm, is the AlgorithmIdentifier parameters field be present, and does the parameters field contain NULL? [RFC 2630 12.3.2.1]		
Do CMS implementations that include symmetric key-encryption key management include Triple-DES key-encryption keys wrapping Triple-DES content-encryption keys [RFC 2630 12.3.3]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
If 128-bit RC2 keys are used as key-encryption keys, is the RC2ParameterVersion parameter set to 58? [RFC 2630 12.3.3]		
In conjunction with key agreement algorithms, do CMS implementations include encryption of content-encryption keys with the pairwise key-encryption key generated using a key agreement algorithm? [RFC 2630 12.3.3]		
For the triple-DES key encryption is the AlgorithmIdentifier parameter field NULL? [RFC 2630 12.3.3.1]		
For RC2 key encryption, is the AlgorithmIdentifier parameter field RC2wrapParameter: RC2wrapParameter ::= RC2ParameterVersion RC2ParameterVersion ::= INTEGER? [RFC 2630 12.3.3.2]		
For RC2 rc2ParameterVersion values of 160, is the value 160 encoded as two octets (00 A0)? (Note that one octet (A0) encoding represents a negative number.) [RFC 2630 12.3.3.2]		
If the key-encryption key is RC2, is it a 128-bit key and is the RC2ParameterVersion parameter set to 58? [RFC 2630 12.3.3.2]		
Does the CMS implementation include Triple-DES in CBC mode for the content encryption algorithm? [RFC 2630 10.1, 12.4]		
Does the CMS implementation also include RC2 in CBC mode for the content encryption algorithm? [RFC 2630 12.4]		
For triple-DES algorithms, is the AlgorithmIdentifier parameters field present, and does the parameters field contain a CBCParameter: CBCParameter ::= IV IV ::= OCTET STRING -- exactly 8 octets? [RFC 2630 12.4.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For RC2 algorithms, is the AlgorithmIdentifier parameters field present, and does the parameters field must contain a RC2CBCParameter: RC2CBCParameter ::= SEQUENCE { rc2ParameterVersion INTEGER, iv OCTET STRING } -- exactly 8 octets? IV ::= OCTET STRING -- exactly 8 octets? [RFC 2630 12.4.2]		
For RC2 rc2ParameterVersion values of 160, is the value 160 encoded as two octets (00 A0)? (Note that one octet (A0) encoding represents a negative number.) [RFC 2630 12.4.2]		
For message authentication code algorithms, if the CMS implementation supports authenticatedData, does it include HMAC with SHA-1? [RFC 2630 10.1, 12.5]		
For HMAC with SHA-1, is the AlgorithmIdentifier parameters field absent? [RFC 2630 12.5.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the CMS implementation include encryption of a Triple-DES content-encryption key with a Triple-DES key-encryption using the following algorithms? The Triple-DES key wrap algorithm is: 1. Set odd parity for each of the DES key octets comprising the content-encryption key, call the result CEK. 2. Compute an 8 octet key checksum value on CEK as described above in Section 12.6.1, call the result ICV. 3. Let CEKICV = CEK || ICV. 4. Generate 8 octets at random, call the result IV. 5. Encrypt CEKICV in CBC mode using the key-encryption key. Use the random value generated in the previous step as the initialization vector (IV). Call the ciphertext TEMP1. 6. Let TEMP2 = IV || TEMP1. 7. Reverse the order of the octets in TEMP2. That is, the most significant (first) octet is swapped with the least significant (last) octet, and so on. Call the result TEMP3. 8. Encrypt TEMP3 in CBC mode using the key-encryption key. Use an initialization vector (IV) of 0x4adda22c79e82105. The ciphertext is 40 octets long. The Triple-DES key unwrap algorithm is: 1. If the wrapped content-encryption key is not 40 octets, then error. 2. Decrypt the wrapped content-encryption key in CBC mode using the key-encryption key. Use an initialization vector (IV) of 0x4adda22c79e82105. Call the output TEMP3. 3. Reverse the order of the octets in TEMP3. That is, the most significant (first) octet is swapped with the least significant (last) octet, and so on. Call the result TEMP2. 4. Decompose the TEMP2 into IV and TEMP1. IV is the most significant (first) 8 octets, and TEMP1 is the least significant (last) 32 octets. 5. Decrypt TEMP1 in CBC mode using the key-encryption key. Use the IV value from the previous step as the initialization vector. Call the ciphertext CEKICV. 6. Decompose the CEKICV into CEK and ICV. CEK is the most significant (first) 24 octets, and ICV is the least significant (last) 8 octets. 7. Compute an 8 octet key checksum value on CEK as described above in Section 12.6.1. If the computed key checksum value does not match the decrypted key checksum value, ICV, then error. 8. Check for odd parity each of the DES key octets comprising CEK. If parity is incorrect, then there is an error. 9. Use CEK as the content-encryption key. [RFC 2630 12.6, 12.6.2, 12.6.3]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For key agreement of RC2 key-encryption keys, are128 bits generated as input to the key expansion process used to compute the RC2 effective key? [RFC 2630 12.6 RFC 2268]		
For both Triple-DES and RC2 key wrap algorithms, when the same content-encryption key is wrapped in different key-encryption keys, is a fresh initialization vector (IV) generated for each invocation of the key wrap algorithm? [RFC 2630 12.6.2, 12.6.4]		
Does the implementation protect the signer's private key? [RFC 2630 Security Considerations]		
Does the implementation protect the key management private key, the key-encryption key, and the content-encryption key? [RFC 2630 Security Considerations]		
Does the implementation protect the key management private key and the message-authentication key? [RFC 2630 Security Considerations]		
Does the implementations randomly generate content-encryption keys, message-authentication keys, initialization vectors (IVs), and padding? [RFC 2630 Security Considerations]		
Does the implementer ensure that key-encryption algorithms are as strong or stronger than content-encryption algorithms? [RFC 2630 Security Considerations]		

Other information:

Findings:

Recommendations for Standards Work: